Application Service Provider Privacy & Security Policies

Access	Security is provided on the data, application and hosting level. The security infrastructure includes a physically secure data center, proven firewall protection, instruction prevention measures, SSL encryption of all data in transit, role based authorization and additional proprietary security measures. The equipment hosting the application is located in a physically secure facility, which requires prior authorization to access the servers. There will be clear decision by company regarding the personnel who will access the sensitive data for various purposes like, migration, client support, issue resolution etc. A non disclosure agreement will be signed with those personnel before entrusting the job.
Authorization	Each client will sign a HIPAA Business Associate Agreement. This agreement guides and authorizes the company employees who are covered under a non disclosure agreement for the physical access of the servers and the databases for various purposes to upkeep the application.
Authentication	Application has two level authentication, windows level and application level. The application level passwords are stored in encrypted formats. 3DES algorithm is used for encrypting and decrypting the password.
Audit	A complete audit of the application transactions is stored in the database.
Secondary Uses of Data	Secondary Use of the PHI data is allowed under an agreement with the client who owns the data. For such usage, sufficient de-identification with no ability for re-identification is done so that privacy is protected.
Data Ownership	Customer owns the data. Company charges the customer for various services provided to the customer in the access of the data in various customer required formats like reports, exporting to different usable formats